

formatting a key exchange response message including the second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

REMARKS

Claims 82-116 remain in this application. Claims 54-81 have been canceled without prejudice. Claim 82 is dependent on a canceled claim, and therefore, has been rewritten in independent form. Claims 84, 88, 89, 96, 98, 99, and 102 have been amended for clarity and to correct minor clerical errors. These amendments do not narrow the scope of the claims and are not being made for reasons of patentability. Claim 103 has been amended to add limitations that bring it within the scope of claim 81. Accordingly, this amendment does not touch on the merits of the case or require a further search to determine patentability. Accordingly, inasmuch as the amendments place the application in better condition for allowance, or for appeal, entry thereof is respectfully requested.

The Patent Office has objected to the drawings for lack of certain labels. In response, Applicant submits herewith proposed drawing corrections in accordance with MPEP § 608.02(v) along with a separate letter to the Official Draftsperson pursuant to MPEP § 608.02(r). Approval of the proposed drawing corrections is respectfully requested. Formal drawings incorporating the proposed corrections will be filed after a Notice of Allowance is received.

Claim 54, 55 and 51 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg (U.S. 6,240,091) in view of Schneier. Claims 56-74 and 82-102 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claims 54, 55 and 81, and further in view of Walker (U.S. 6,263,438). Claims 75-80 and 103-116 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier and Walker as applied to claim 54, and further in view of Thompson (U.S. 6,282,552). With respect to

canceled claims 54-80, these rejections are moot. With respect to claims 81-116, Applicant respectfully traverses these rejections.

The novelty of Applicant's approach does not merely reside in the use of public key cryptography by a smartcard or its equivalent, or in the use of mutual authentication, or in the use of session keys during transactions. The present invention does not use any of the existing concepts of 'public key infrastructure' or certificates, nor does not use any prearranged shared secrets between any transacting parties, nor does it use key databases or central key servers for any purposes. The present invention needs to be viewed as a whole, not in piecemeal. The present invention, when viewed as a whole, is a cryptographic system and method that is a novel, unobvious, secure and efficient way to conduct transactions using a public network such as the Internet. From this perspective, claims 81-116, as a whole, are clearly distinguishable from Ginzboorg and Schneier.

The present invention, when viewed as a whole, includes the following features:

- (1) Only two parties are involved in a transaction (e.g., a cardholder and a service provider);
- (2) The cardholder obtains the public key of the service provider and makes it available on the smartcard. This information by definition is public and the cardholder can obtain it in any manner.
- (3) The cardholder, under the protection of the service provider's public key, starts a key exchange sequence with the service provider. With this protection, the two parties can do the mutual authentication and key exchange simultaneously.
- (4) During the key exchange sequence, a session key is generated by the service provider, and is securely passed to the cardholder, and is properly verified by both parties following a successful exchange of the session key.
- (5) The subsequent transaction is carried out under the protection of the newly established session key for this specific transaction.

There are a number of components of the cryptographic system that do not appear to have been considered by the Patent Office.

- (1) The transaction is carried out between two parties, the cardholder and the service provider. In Schneier's system, three parties are involved - Alice, Bob, and Trent. Trent has paramount importance in Schneier's system - everybody in the system must have Trent's public key and Trent has everybody's public key; all transactions are 'pre-registered' with Trent; and Trent assigns the session keys to all transactions. Without Trent, nothing works in Schneier's system. None of these functions are needed in the present invention.
- (2) Schneier does not teach how Trent can be set up initially and how the different parties can 'pre-register' each transaction with him.
- (3) Ginzboorg is limited to the use of another party's public key for key signature verification purpose. The use of the second party's public key in the present invention goes far beyond that.

In the Office action, the Patent Office admits that the combination of Ginzboorg and Schneier does not teach sending the cardholder's public key to the server provider. Instead, the Patent Office relies on Walker for teaching a digital certificate. The Patent Office takes the position that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send a certificate with Alice's first message, as taught by Walker et al., to provide greater assurance." Applicant responds as follows:

- (A) It is not clear which message the Patent Office is referring to - the first message from Alice to Trent or the first message from Alice to Bob. But either way, the person of ordinary skill would be making a useless, if not erroneous, step. First, Trent already has Alice's public key, he doesn't need her certificate and he has no way of verifying it anyway. Second, Bob gets Alice's public key from Trent. He cannot and will not accept a certificate which he cannot verify. If he does accept the certificate and no


longer uses Trent for this purpose, then the integrity of Schneier's system would be compromised rendering it vulnerable to security breaches.

- (B) A certificate requires a signing authority and has an expiration date. The use of a certificate requires a complicated relationship of trust, as well as a complicated support structure. One of the advantages of Applicant's approach is that a certificate is not required.

In view of the foregoing remarks, it is clear that the present invention is not disclosed by the combination of references cited by the Patent Office. Accordingly, Applicant respectfully submits that this application is now in condition for allowance, and reconsideration and allowance are respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,


Craig A. Gelfound
Registration No. 41,032

MCDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
(310) 277-4110
Facsimile: (310) 277-4730
Date: May 27, 2003

APPENDIX A

Claims 82, 84, 88, 89, 96, 98, 99, 102 and 103 have been amended as follows:

82. (Amended) A [The] method of [claim 81 wherein] conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at a member, the key exchange request message having [includes] a public key of the member, and at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

generating a session key at the service provider in response to the key exchange request message;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to complete the transaction.

84. (Amended) The method of claim 82 or 83 wherein the use of [using] the session key to complete the transaction comprises:

formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

88. (Amended) The method of claim 84 wherein the transaction request message comprises the response to the [a] service provider challenge.

89. (Amended) The method of claim 84 wherein the transaction response message includes data encrypted with the session key [a portion of the data].

96. (Amended) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

- generating a member challenge by a [the] member;
- encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;
- formatting by the member a key exchange request message including the first cryptogram and a public key of the member;
- signing digitally by the member the key exchange request message;
- sending the digitally signed key exchange request message to the service provider;
- generating by the service provider a service provider challenge;
- generating by the service provider a session key;
- encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;
- formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge;
- signing digitally by the service provider the key exchange response message;
- sending the digitally signed key exchange response message to the member;
- encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;
- attaching the third cryptogram to a transaction message going from the member to the service provider;
- signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message [going] from the member to the service provider [to the service provider].

98. (Amended) The method of claim 96 wherein the key exchange request message comprises the member's [cardholder's] public key encrypted with the service provider's public key.

99. (Amended) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting the member [a cardholder] challenge response as part of the second cryptogram.

102. (Amended) The method of claim 101 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the member [cardholder location] to the service provider [location].

103. (Amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating a first session key at the service provider in response to the first key exchange request message;

generating a second session key at the service provider in response to the second key exchange request message;

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including the [a] second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

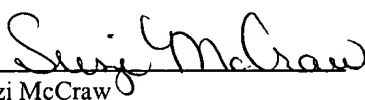
separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.



2132
#14
6-10-03
SM

PATENT
064808-0011

I certify that on May 27, 2003, which is the date I am signing this certificate, this correspondence and all identified attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop PGPUB Drawings, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.


Suzi McCraw

Applicant: Jay C. Chen

Serial No.: 09/456,794

Filed : December 8, 1999

Title: A CRYPTOGRAPHIC SYSTEM
AND METHOD FOR
ELECTRONIC TRANSACTION

Examiner: Meislahn, Douglas

Group/Div.: 2132

Approved
6/17/03

LETTER TO OFFICIAL DRAFTSPERSON

Mail Stop PGPUB Drawings
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED

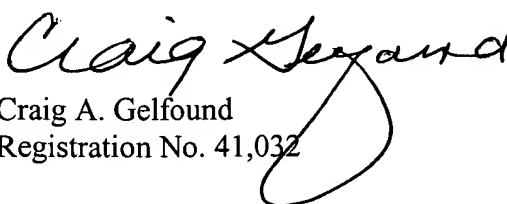
JUN 03 2003

Technology Center 2100

Commissioner:

Pursuant to MPEP § 608.02(r), applicant submits herewith two (2) sheets of proposed drawing corrections, showing FIG. 2 and FIG 12 marked in red ink. Approval of these drawing corrections is respectfully requested.

Respectfully submitted,


Craig A. Gelfound
Registration No. 41,032

Date: May 27, 2003

MCDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
(310) 277-4110
Facsimile: (310) 277-4730

FIG. 2

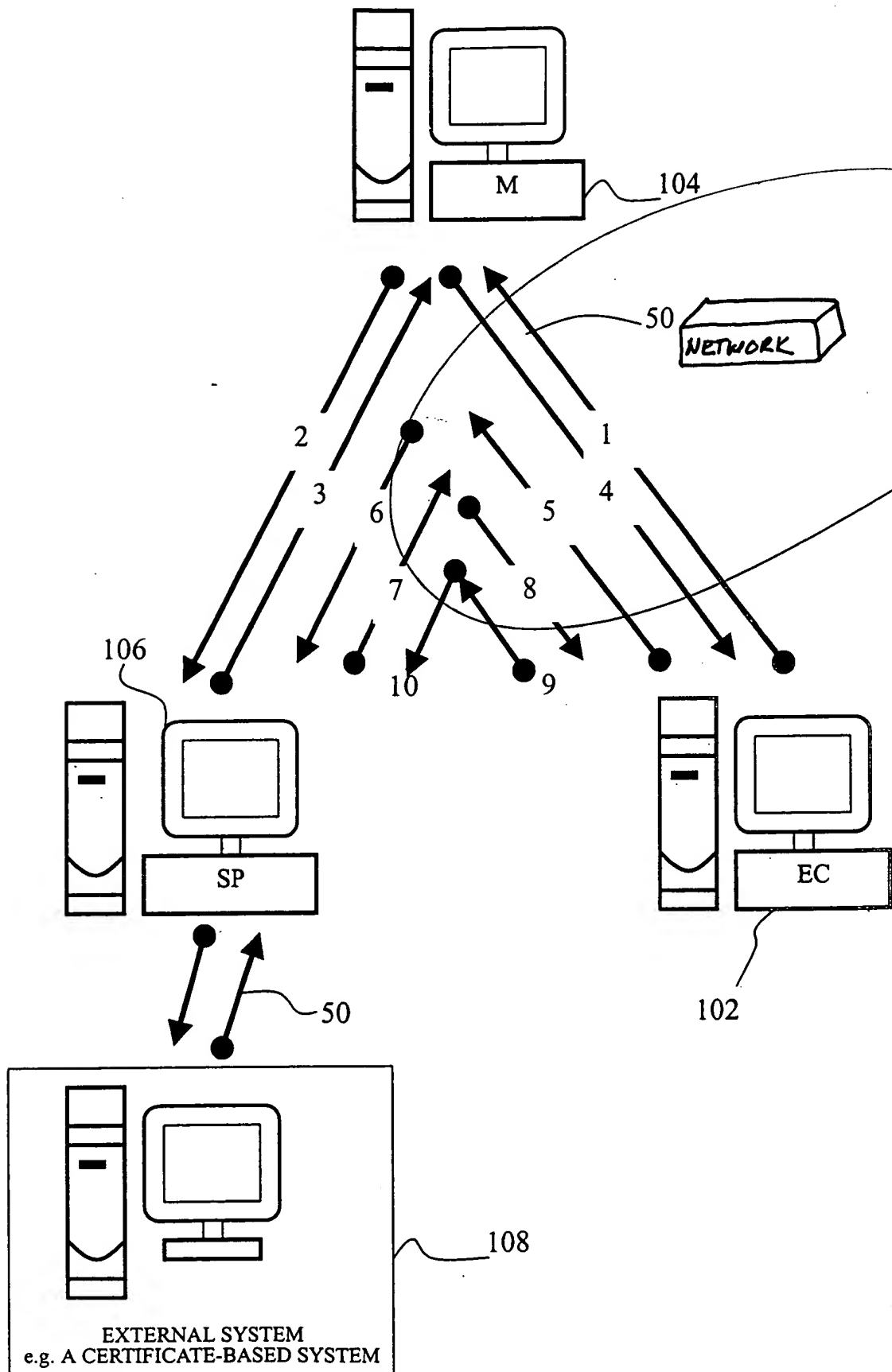


FIG. 12

